Abstract of the Disclosure

Linux's NAT (Network Address Translator) implementation, IP Masquerade, includes a VPN Masquerade feature that provides interoperation of NAT with IKE and ESP tunnel mode within the IPSec security protocol suite. VPN Masquerade uses heuristics to route packets from a server on the Internet to a client on a local network that shares access to the Internet with other clients over a common access link through a router running NAT. VPN Masquerade, however, is susceptible to crashes, collisions and race conditions that can disable IPSec communication. These are prevented, or recovery from such is automatically effected, by sending over a tunnel a control packet, a "ping", from the client at one end of the tunnel to the server at the other end of the tunnel, and then waiting to send any packets other than a control packet over the tunnel until a responsive control packet is received from the server. The tunnel is defined by an epoch that comprises one security association (SA) in each direction that has a negotiated limited lifetime and defines the use of the ESP protocol in tunnel mode with negotiated authentication and/or encryption keys and a security parameters index (SPI) chosen by the SA's destination. If the client does not receive a response to the "ping" within a predetermined time, then it re-"pings" the server up to a predetermined number of times and, if no response is received, rekeys the tunnel. Further, the client "pings" the server if no packet is received on a tunnel for a predetermined period of time. By also configuring the server to wait to switch to a new epoch until it receives a "ping" from a client, certain race conditions can be eliminated. Alternatively, the client can be configured to ignore an attempt by the server to start a negation for rekeying the tunnel. Automatic recovery from a crash of the NAT is also provided by automatically starting a new IKE session if attempts to rekey a tunnel are not successful.